RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: PART1-W01

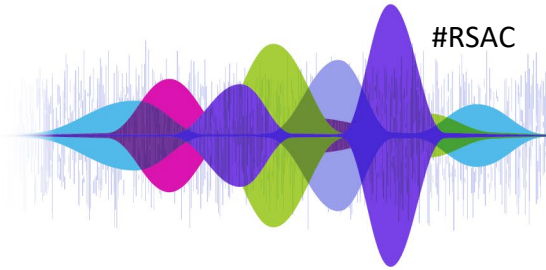
Revisiting Layered Security: A Robust Approach to Blocking Network Threats

Senthil Ramakrishnan

AVP Product Management & Dev Cybersecurity
AT&T Business / Network Security
www.linkedin.com/in/senthil-ramakrishnan-66406b30/

Will Amores

Director Product Management & Development
AT&T Business / Network Security
www.linkedin.com/in/will-amores/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Today's Challenges

Cloud-first approach is fueling internet connectivity

As 5G and fiber are growing, your threat surface is also expanding

Digital transformation is top of mind

Need solutions that support growth strategies and the ability to scale quickly

Attacked from all sides*

The cyberthreat landscape is ever-evolving and expanding

Limited resources available to manage and maintain policies and controls

*Gartner 2021 Global Security and Risk Management Survey

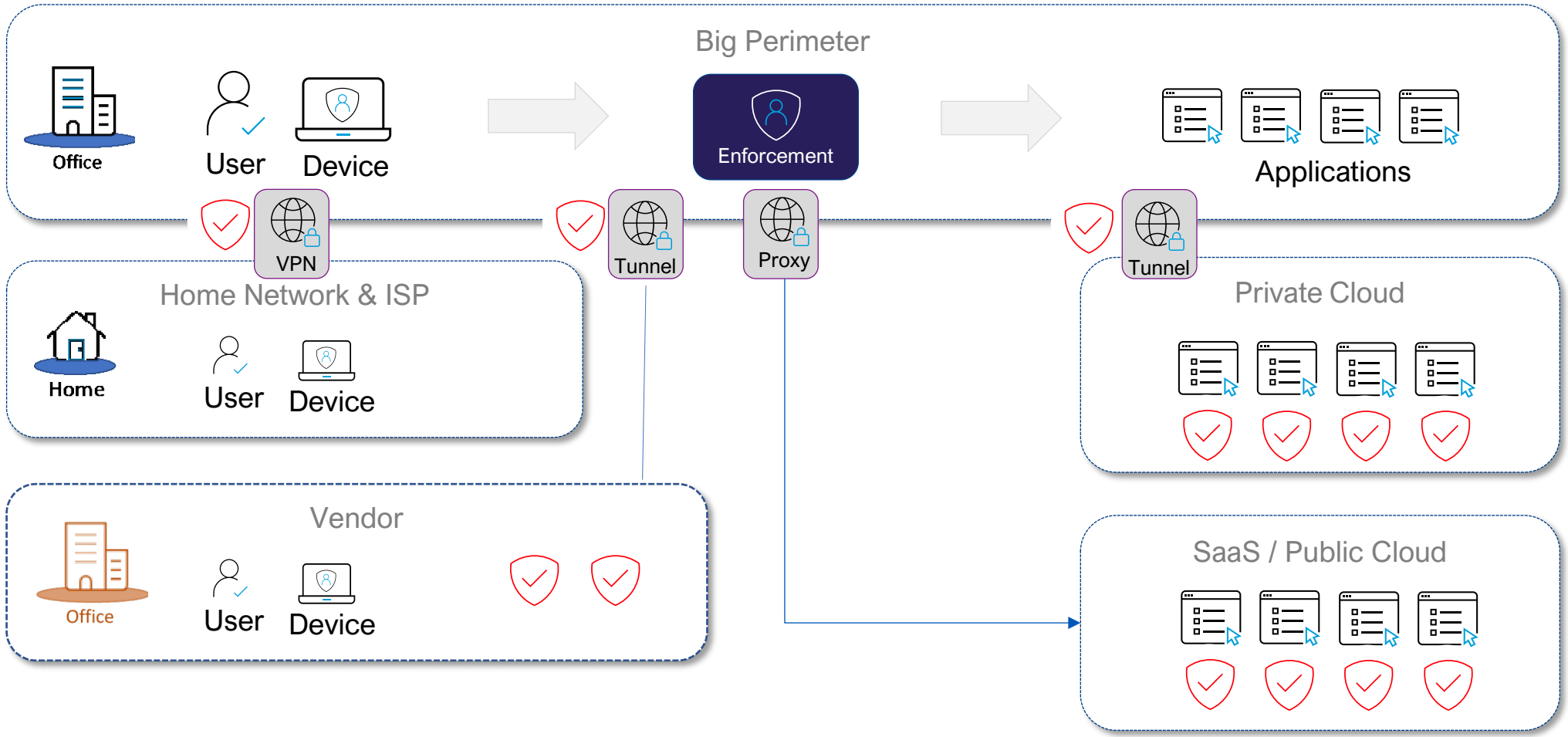
Complexity is a challenge

Lack of expertise to manage and maintain multiple security solutions from multiple vendors

Budget constraints make multiple security solutions too costly

Remember when life was simple…

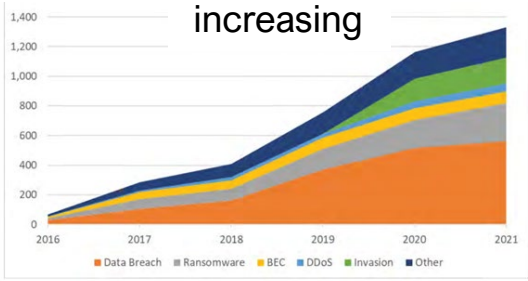
Security has become complex and hard to manage



Cyberattacks affect all

Last year, **181** ransomware attacks involving **25.6 million** healthcare records

K-12 Cyber Incidents are increasing



71% **retail** organizations suffered a breach

Manufacturing took **279** days average before **data breach** is identified

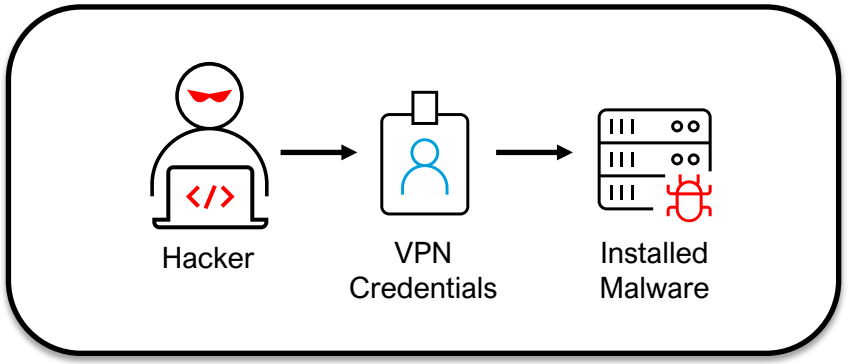
Over **$4B** total money **lost** in investment sector due to cybercrime

Sources:

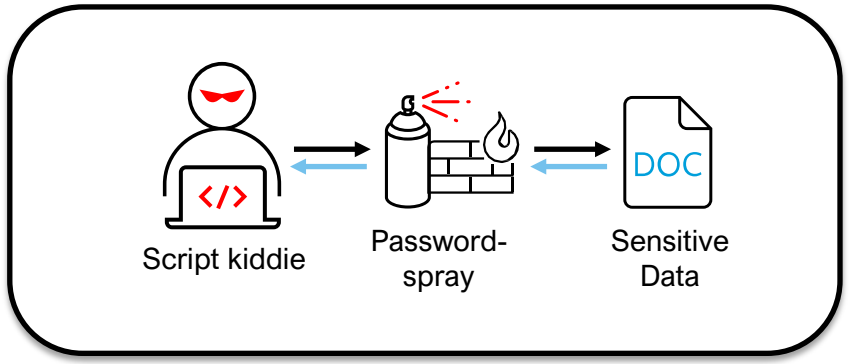
https://www.k12six.org/the-report
https://www.hipaajournal.com/2024-was-another-bad-year-for-healthcare-ransomware-attacks/
https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs
https://securityintelligence.com/articles/cost-of-a-retail-data-breach/
https://securityintelligence.com/articles/addressing-growing-concerns-cybersecurity-in-manufacturing/

Security tools are under attack

- Malicious actors can choke a firewall to break down barrier
- 95% of ransomware attacks were able to bypass firewalls
- 77% successfully circumvented email filtering systems



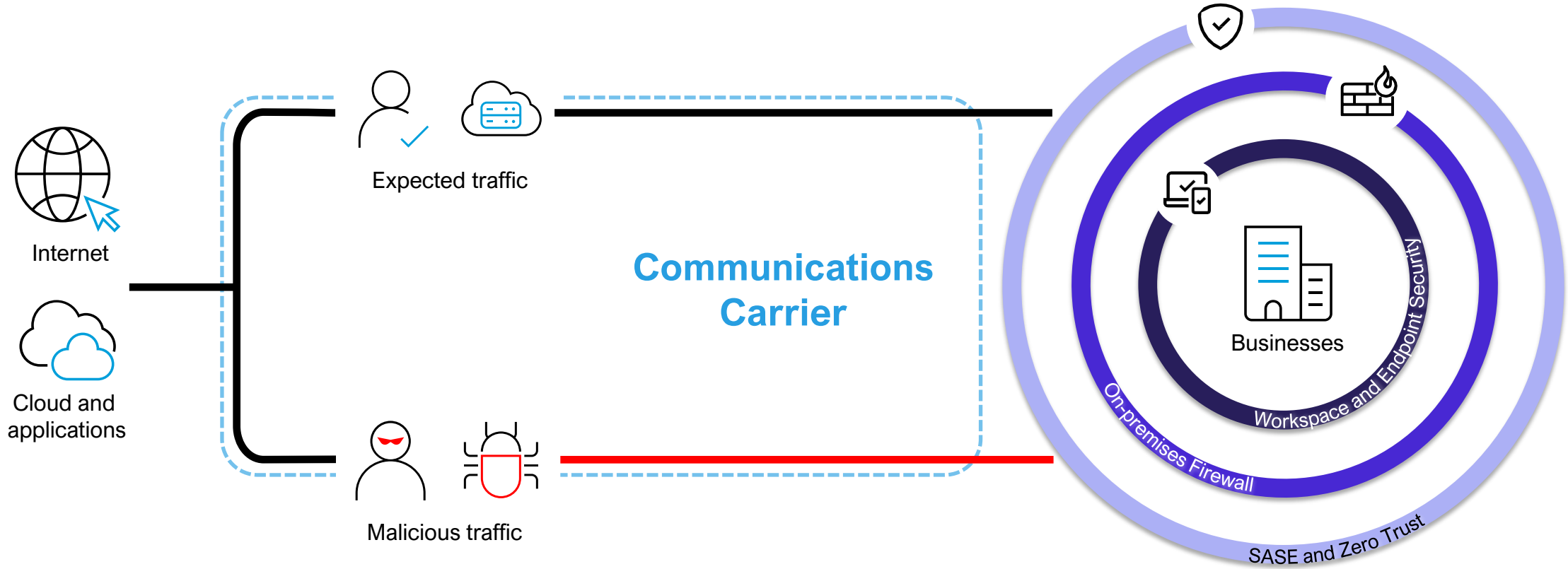
Attackers gained **VPN credentials**, conducted a network scan and **installed malware**



Script kiddie hacker launched a password-spray attack to steal **sensitive data**

Sources:
https://www.varinsights.com/doc/of-ransomware-bypass-firewalls-email-filtering-0001
https://www.helpnetsecurity.com/2020/07/02/cyberattacks-bypass-waf/

Defenses used today



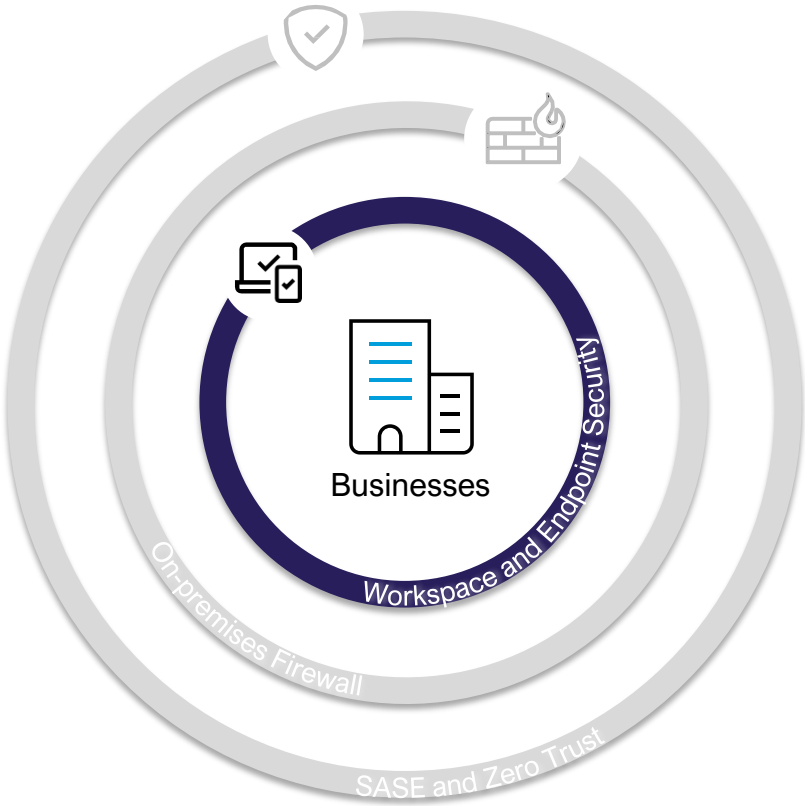
Workspace and Endpoint Security

Benefits

- Protection from Cyber Threats
- Data Loss Prevention
- Compliance with Regulations

Key Components

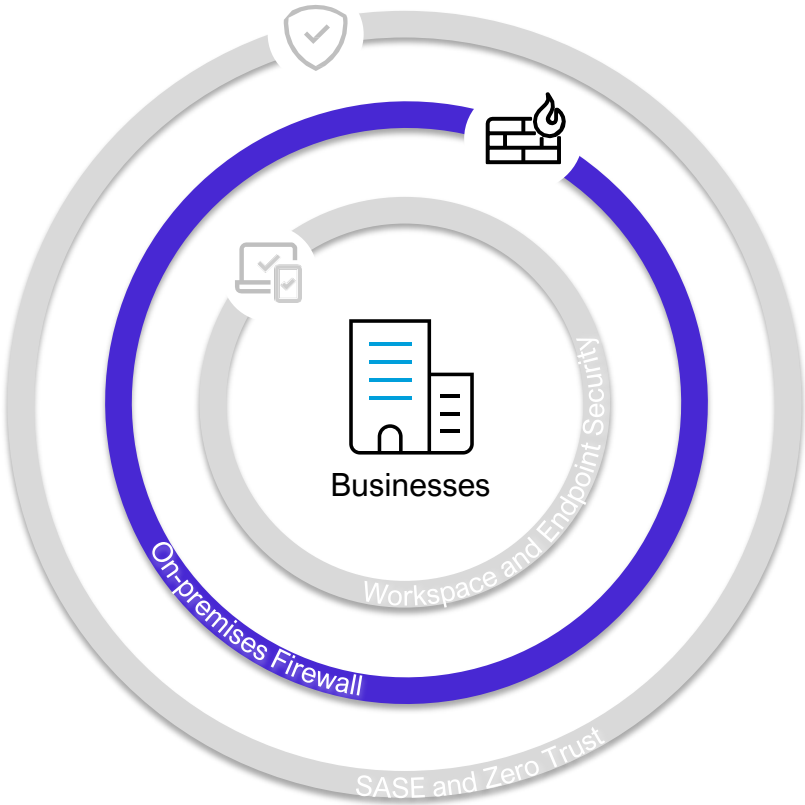
- Antivirus and Anti-Malware
- Detection and Response
- Patch Management



On-premises Firewall

Benefits
- Enhanced Control
- Reduced Latency
- Data Privacy

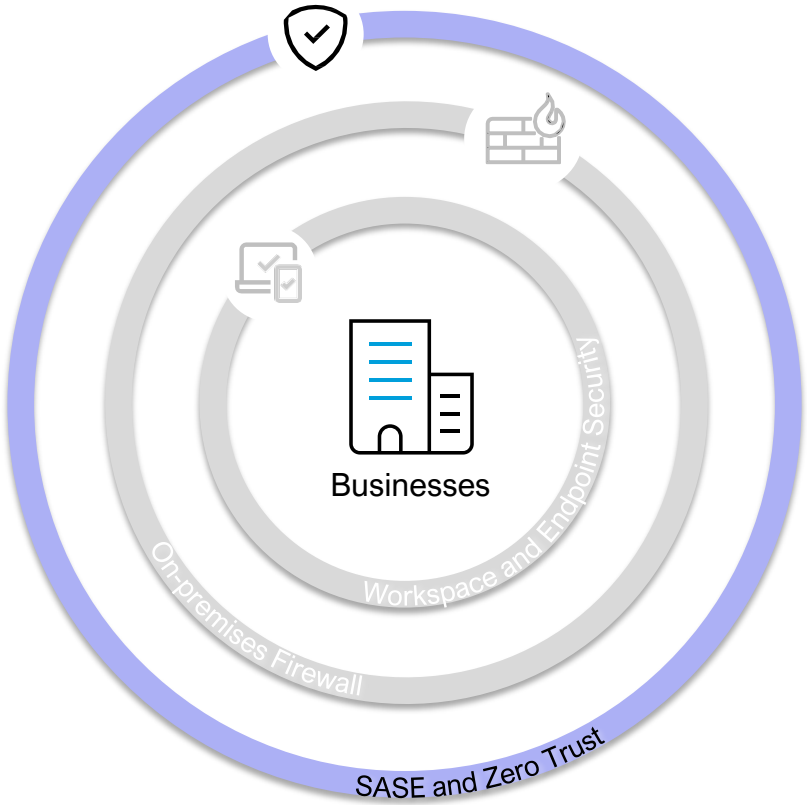
Key Features
- Intrusion Detection and Prevention
- Deep Packet Inspection
- User and Application Control



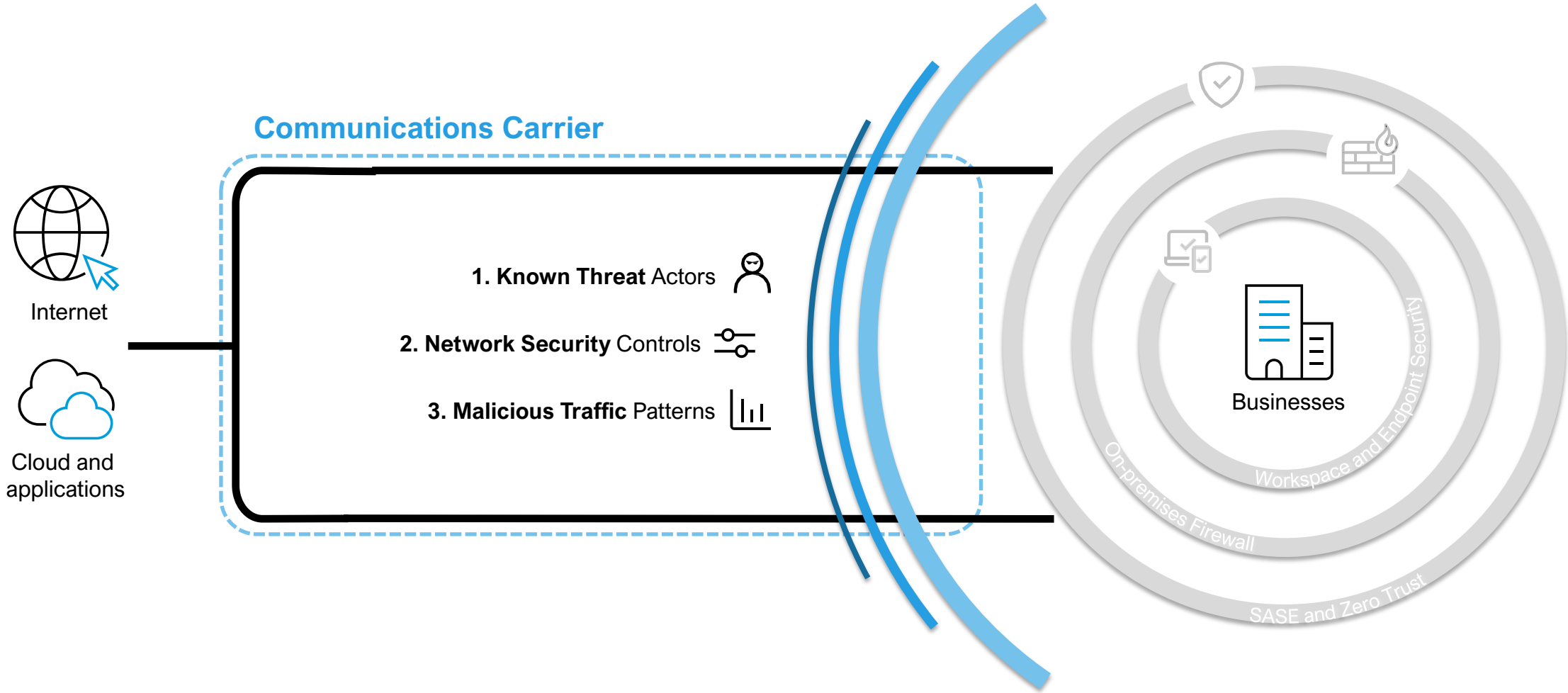
SASE and Zero Trust

Benefits of SASE
- Unified Security Framework
- Enhanced Performance
- Scalability and Flexibility

Principles of Zero Trust
- Verify Explicitly
- Least Privilege Access
- Continuous Monitoring & Assessment



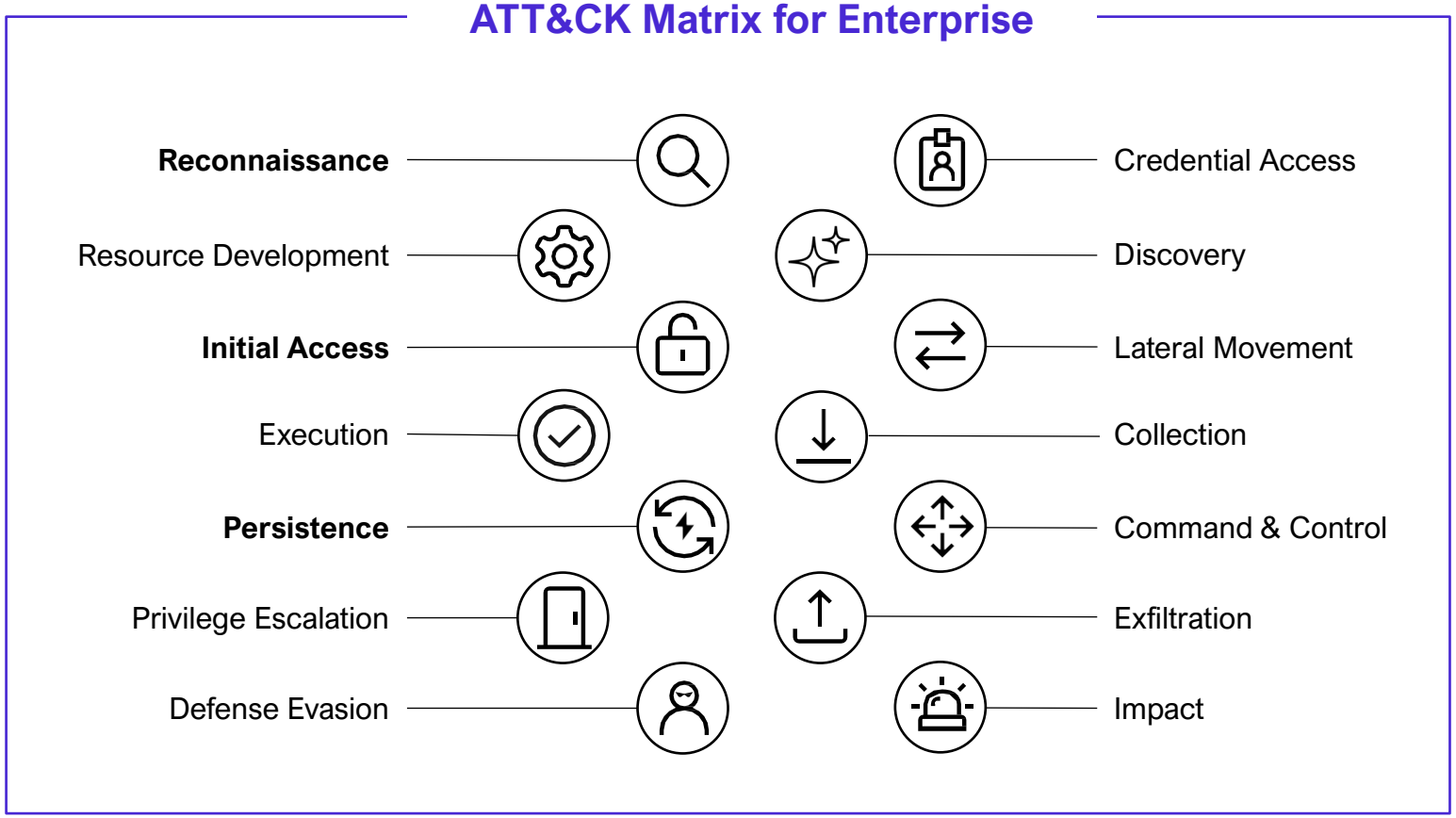
A new layer of defense



First Line of Defense

Network Layer

- Filter traffic in-network (First Contact)
- Detect threats BEFORE they reach the business
- Defeat Reconnaissance and Initial Access Techniques
- Detect and Mitigate Persistence Techniques
- Execute security controls to mitigate threats



Known Threat Actors

Key Threat Sources
- Known Botnets
- Malicious Scanners
- Authentication Abusers

Techniques and Measures
- Machine Algorithm Finds
- Web Application Firewalls
- Honeypot Tracking

Network Security Controls

Network Filters
- Geography
- Web Domains
- Ports and Protocols

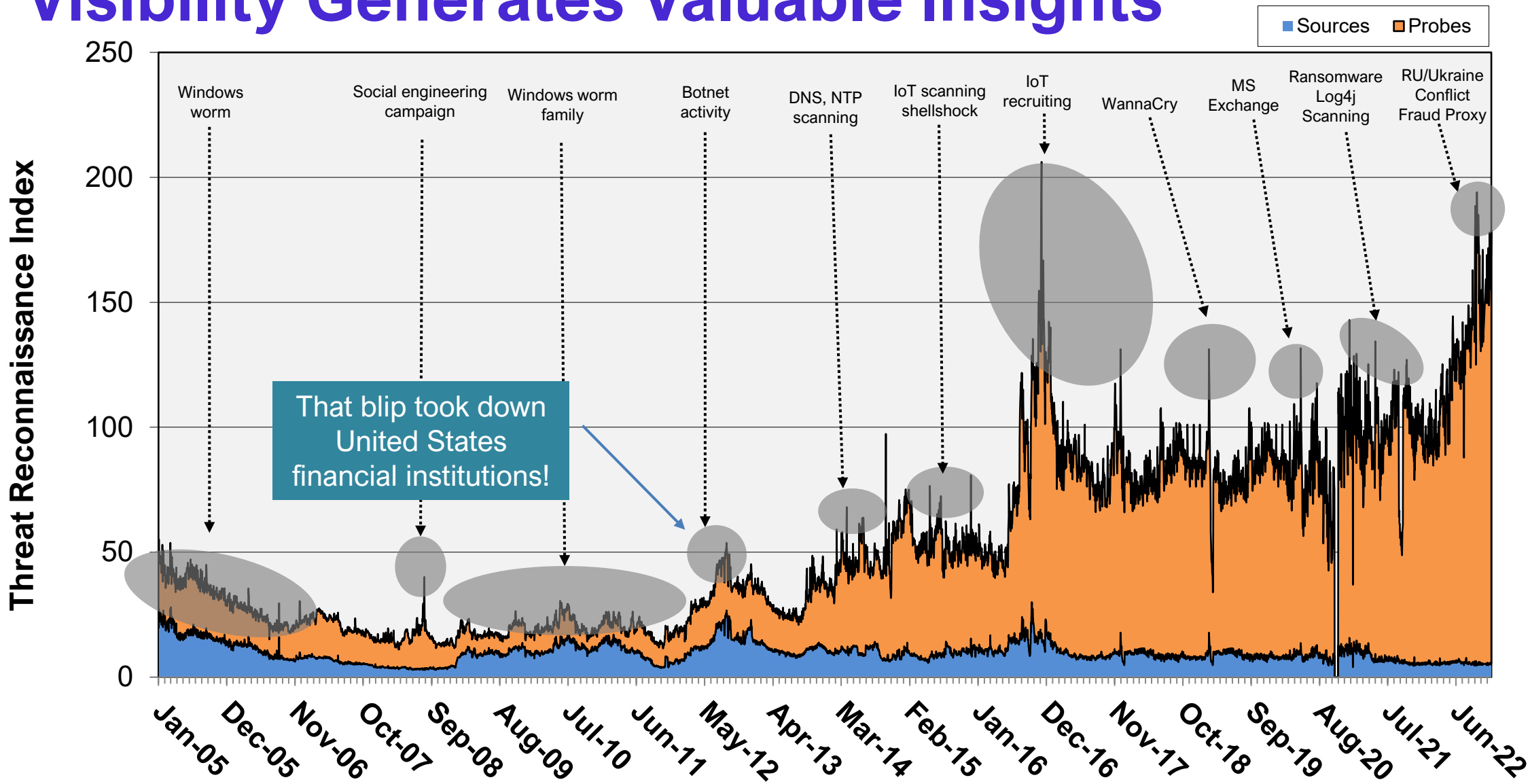
Advanced Controls
- Firewall Rules
- Applications
- Data flows

Malicious Traffic Patterns

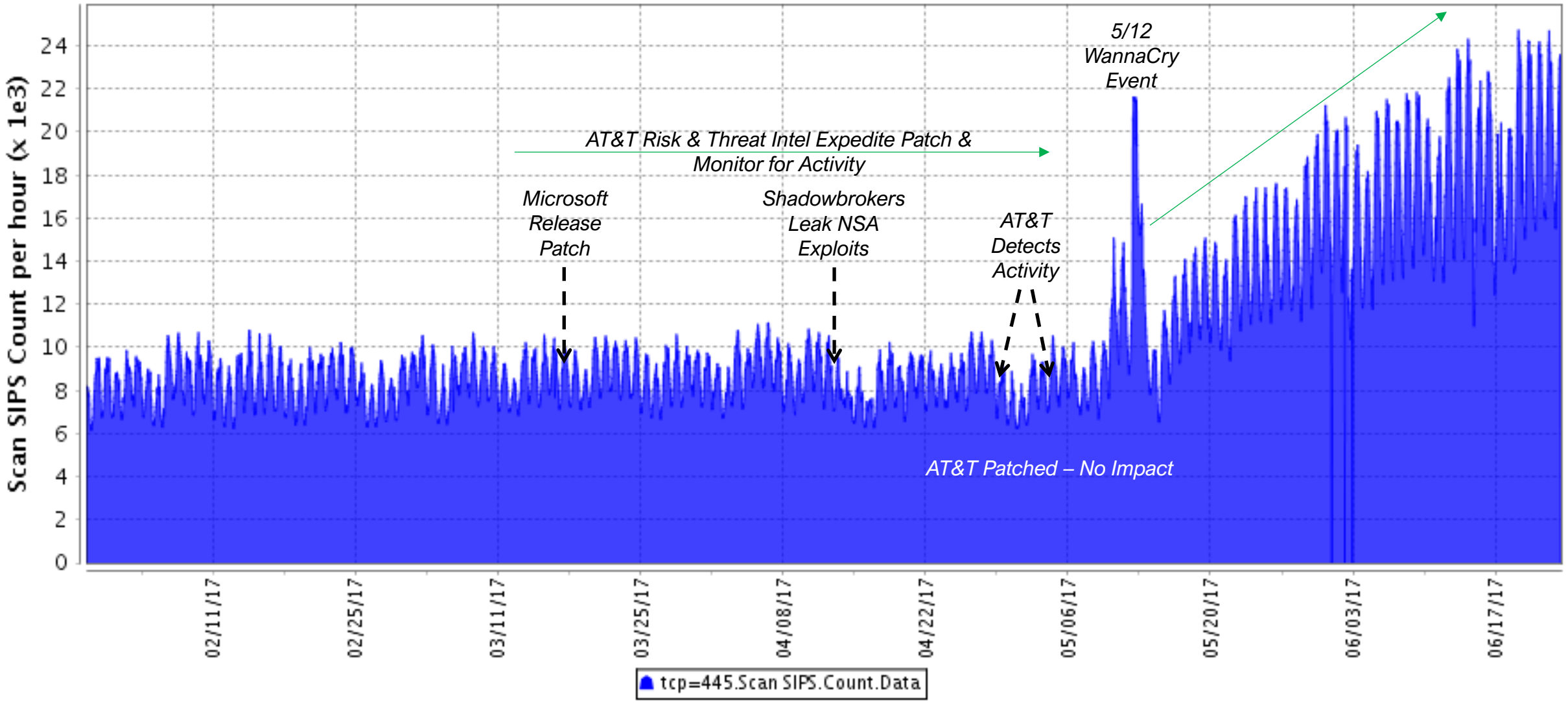
Heuristics methods to analyze network flows:

- Virus
- Malware
- Spyware
- Vulnerability exploits
- IP Anonymizers
- Harmful domains

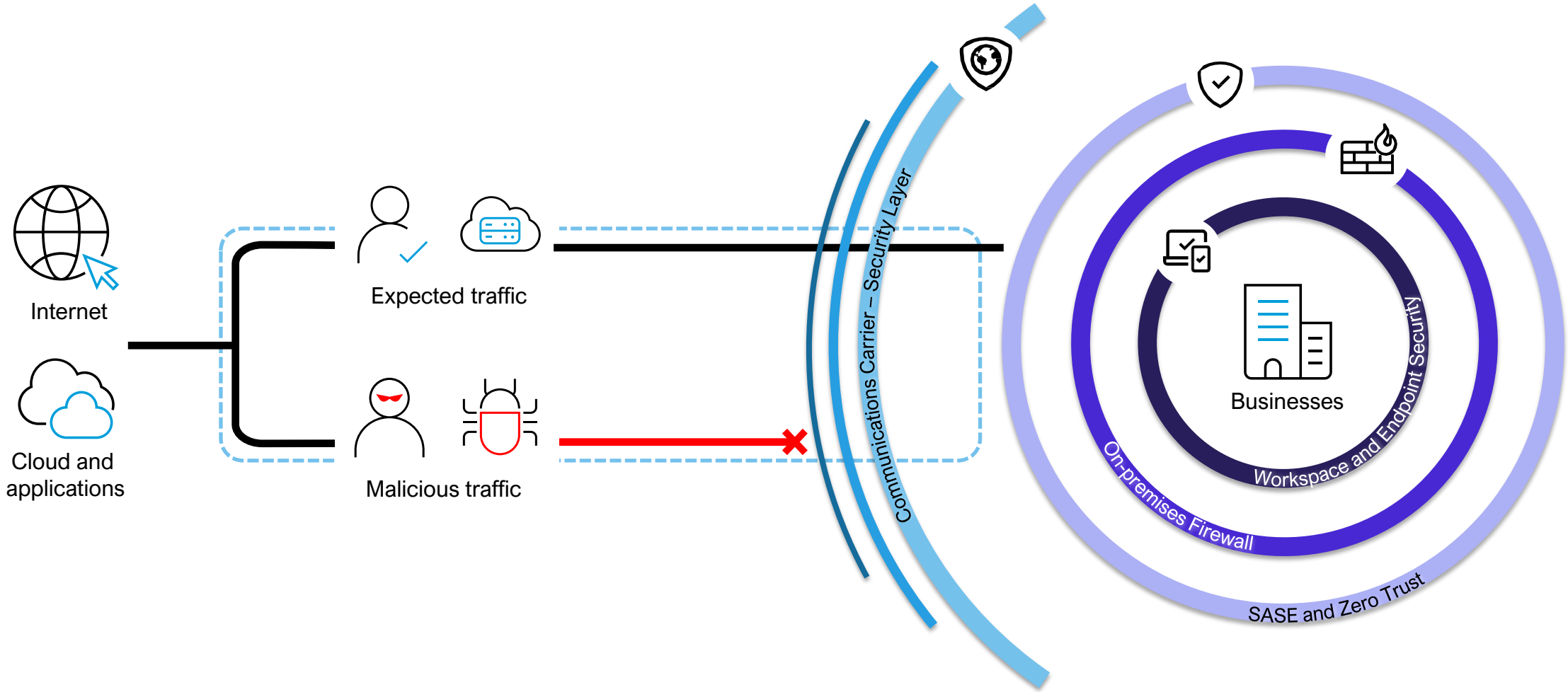
Visibility Generates Valuable Insights



A deeper look at Exploit Activity – WannaCry

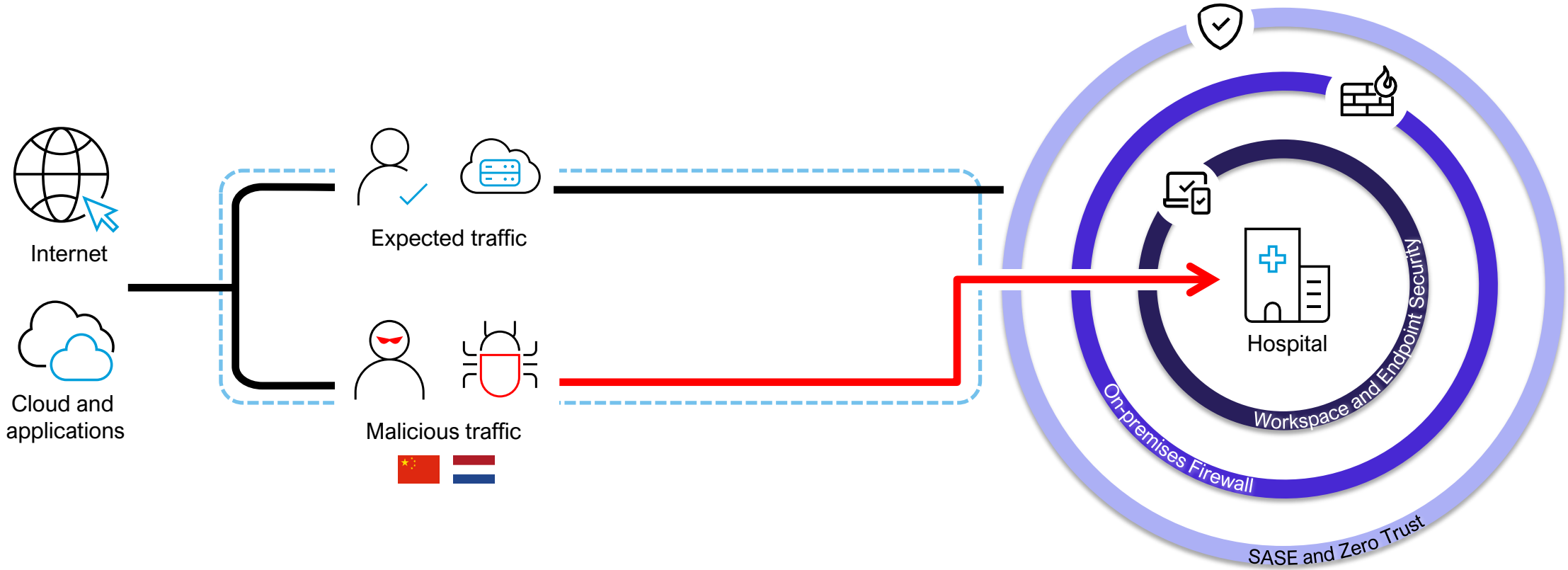


Security layers to mitigate threats



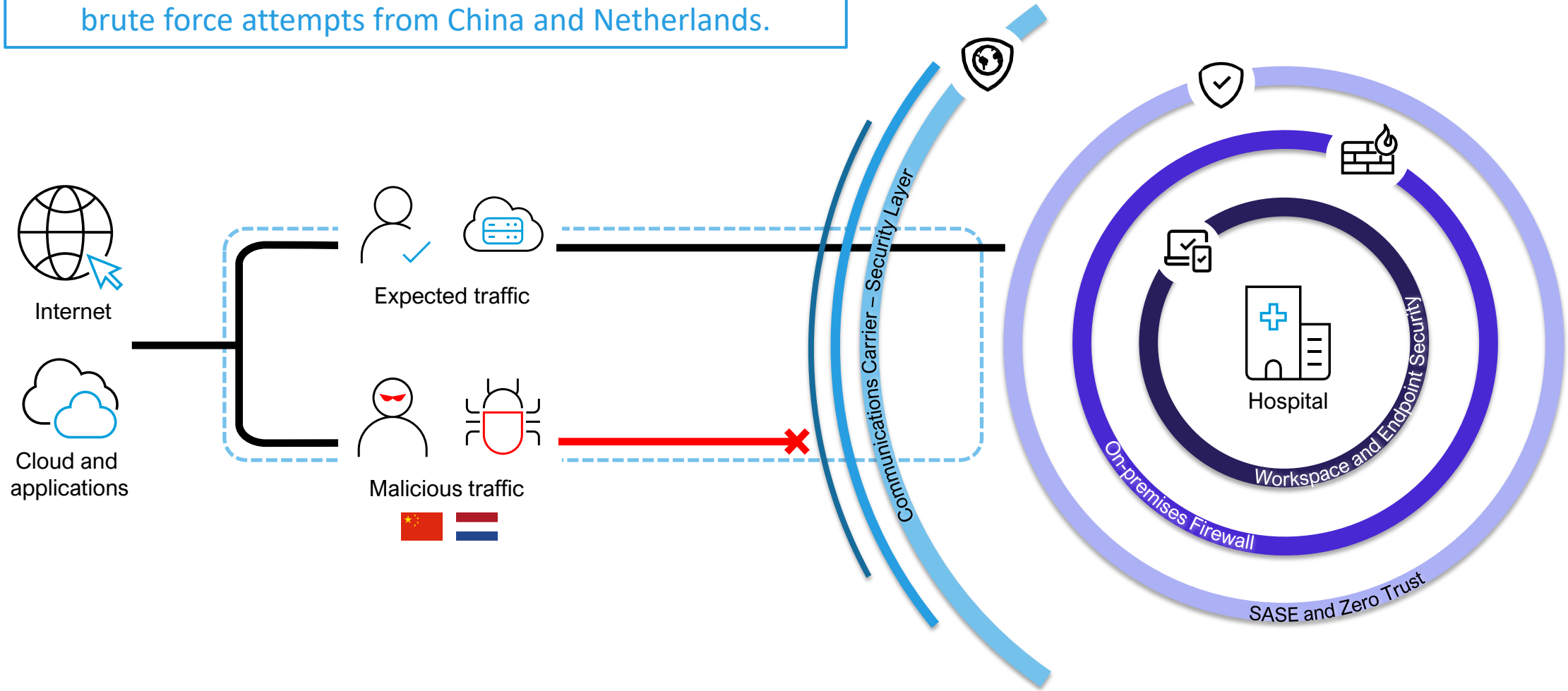
Hospital Example

Brute force attacks from China and Netherlands overwhelmed the firewall. Hospital internet connection and apps hampered.



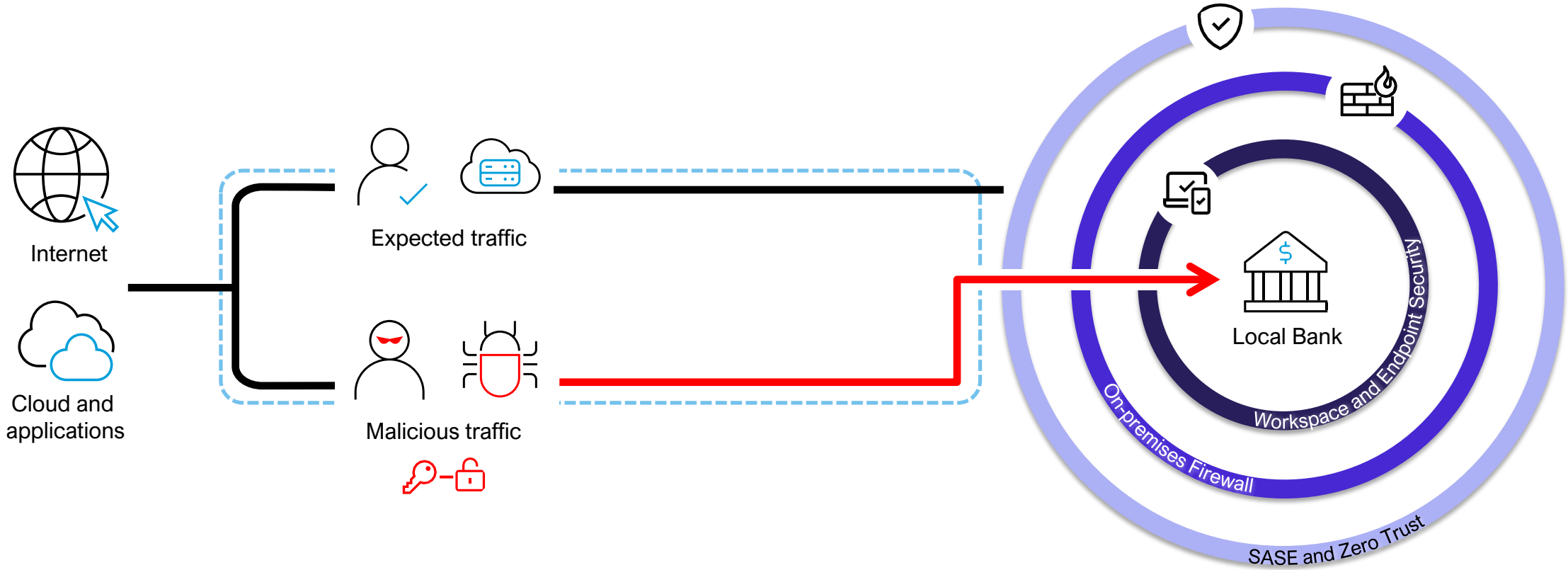
Hospital Example

Hospital used their carrier's security controls to block brute force attempts from China and Netherlands.



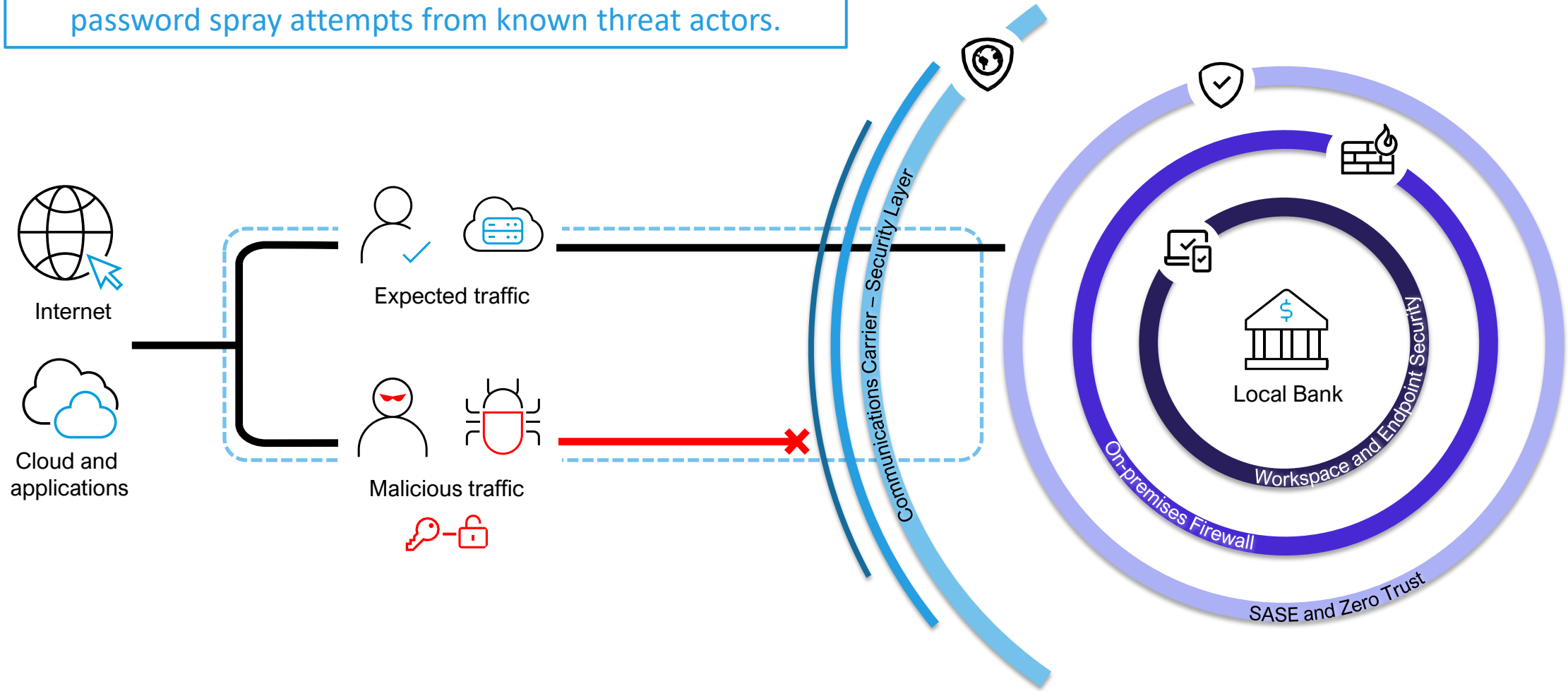
Local Bank Example

Password spray exploiting tunnel vulnerabilities locking up the VPN.
Slowed down financial transactions within the network.

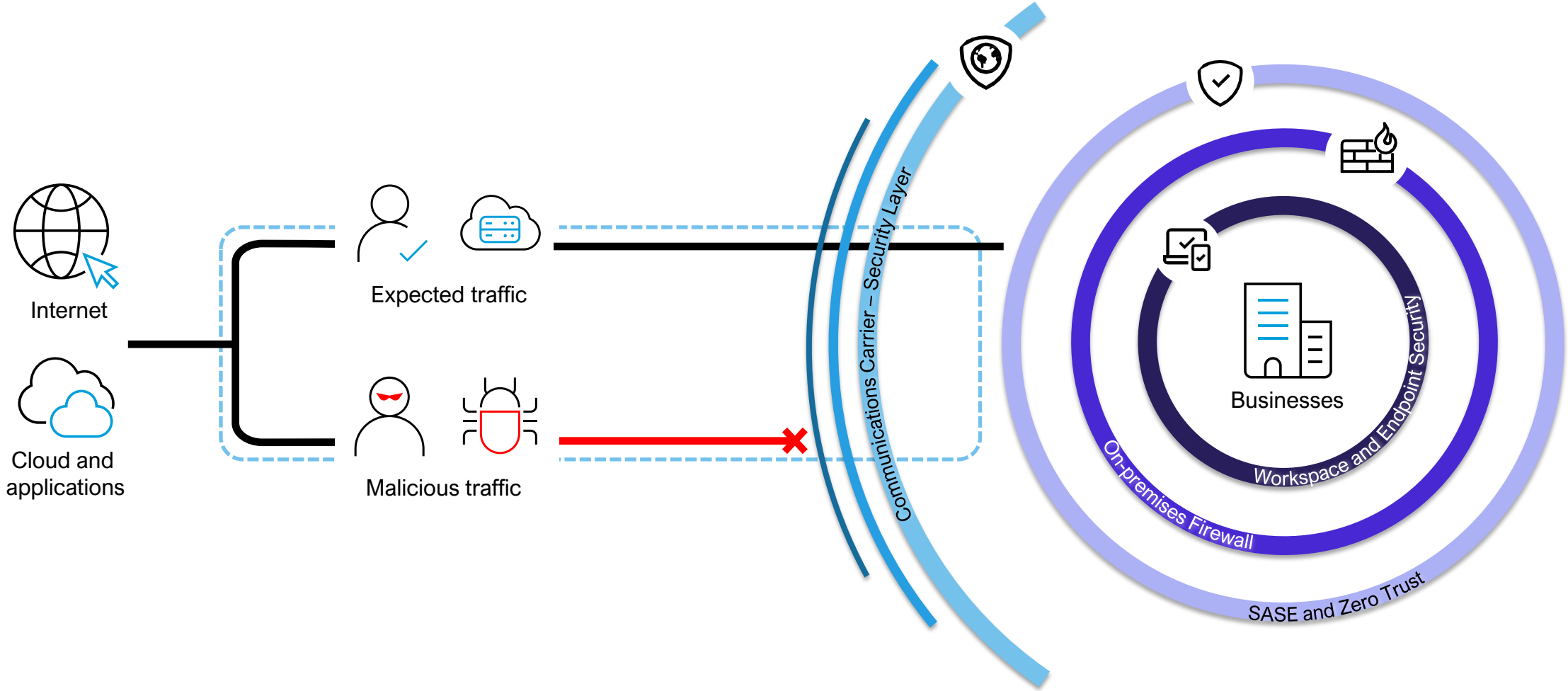


Local Bank Example

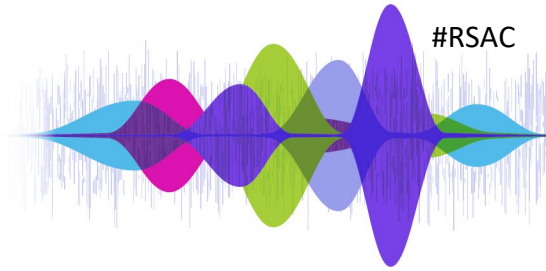
Local bank used their carrier's security controls to block password spray attempts from known threat actors.



Layered Security: A Robust Approach to Blocking Network Threats



Next Steps for Security Leaders



Monday morning

- **Identify** the different security layers deployed in your environment.
- **Assign** a team to assess any potential gaps in the network.

Next 90 days

- **Develop** a strategy to mitigate risks from any interim gaps.
- **Build** a plan to acquire necessary tools to establish a robust layered security.

Next 12 months

- **Provide** stakeholders update on the new layered security approach.
- **Implement** new rules and policies to maximize a defense in depth strategy.

RSAC™ 2025 Conference

Q & A

Many Voices.
One Community.

RSAC 2025 Conference

Many Voices.
One Community.

Thank you!

For more information:

Please visit us in the Expo Hall

AT&T Business N-5770